KRISHNASAMY
College of
ENGINEERING & TECHNOLOGY
Approved by AICTE & Affiliated to Anna University

Anand Nagar, Nellikuppam Main Road, S. Kumarapuram, Cuddalore - 607 109, Tamil Nadu.

☎ (04142) 285 601 - 604   ⊕ www.kcet.in   ⊠ info@kcet.in

DEPARTMENT OF MCA

20.07.2023

CIRCULAR

Ref.: KCET/MCA/VAC/CIRCULAR/2022-23/02.

The following Value Added Course will be conducted during the academic year 2022-2023. The course will be conducted from 02.08.2023 to 08.08.2023. Students are instructed to register their names in the course allotted to them.

Note: Students are instructed to attend the program without fail.

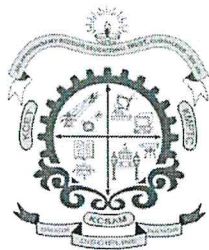| S.No.	Course Code	Name of the Course	Year / Sem	No. of Period	Course Coordinator
1	MCA-VAC2202	Cryptography & Network security	II/III	30	Mr.R.Sathish Kumar, AP/MCA

HoD/MCA
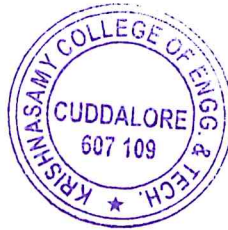
Copy to:

Class Room

Class In charge

Department File

KRISHNASAMY
College of
ENGINEERING & TECHNOLOGY
Approved by AICTE & Affiliated to Anna University

Anand Nagar, Nellikuppam Main Road, S. Kumarapuram, Cuddalore - 607 109, Tamil Nadu.
☎ (04142) 285 601 - 604   ⊕ www.kcet.in   ⊠ info@kcet.in

DEPARTMENT OF MCA

Subject Code: MCA-VAC2202

Subject Name: CRYPTOGRAPHY AND NETWORK SECURITY

Duration: 30 Hours

OBJECTIVES:

- To understand Cryptography Theories, Algorithms and Systems.
- To understand necessary Approaches and Techniques to build protection mechanisms in Order to secure computer networks.

MODULE- I   INTRODUCTION

Security trends – Legal, Ethical and Professional Aspects of Security, Need for Security at Multiple levels, Security Policies – Model of network security – Security attacks, services and mechanisms – OSI security architecture.   6

MODULE- II   SYMMETRIC KEY CRYPTOGRAPHY

SYMMETRIC KEY CIPHERS: SDES -Block cipher Principles of DES – Strength of DES – Differential and linear cryptanalysis – Block cipher design principles – Block cipher mode of operation – Evaluation criteria for AES.   6

MODULE- III   PUBLIC KEY CRYPTOGRAPHY

ASYMMETRIC KEY CIPHERS: RSA cryptosystem – Key distribution – Key management – Diffie Hellman key exchange.   6

MODULE- IV   MESSAGE AUTHENTICATION AND INTEGRITY

Authentication requirement – Authentication function – MAC – Hash function – Security of hash function and MAC – SHA –Digital signature and Authentication protocols.   6

MODULE- V   NETWORK SECURITY

SSL - SSL Architecture, SSL Protocols, SSL Message, Secure Electronic Transaction (SET). TLS – TLS Protocols, DTLS Protocols, PKI – Fundamentals, Standards and Applications.   6

TOTAL: 30 PERIODS

OUTCOMES:

- Understand the fundamentals of networks security, security architecture, threats
- Apply the different cryptographic operations of symmetric cryptographic algorithms
- Apply the different cryptographic operations of public key cryptography
- Apply the various Authentication schemes to simulate different applications.
- Understand various Security practices and System security standards

REFERENCES:

1. William Stallings, "Cryptography and Network Security – Principles and Practice", Seventh Edition, Pearson Education, 2017.
2. Nina Godbole, Sunit Belapure, "Cyber Security: Understanding Cybercrimes, Computer Forensics and Legal Perspectives", First Edition, Wiley India, 2011.

HoD/MCA